



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 09/939,896 | 08/27/2001 | Lane W. Lee | M-12042 US | 4074 |

7590 04/22/2004

MACPHERSON KWOK CHEN & HEID LLP
1762 TECHNOLOGY DRIVE
SUITE 226
San Jose, CA 95110

EXAMINER

BAYAT, BRADLEY B

ART UNIT

PAPER NUMBER

3621

DATE MAILED: 04/22/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. 09/939,896 | Applicant(s) LEE ET AL. |
|------------------------------|--------------------------------------|-----------------------------------|
| | Examiner Bradley Bayat | Art Unit 3621 |

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 27 August 2001.

2a) This action is **FINAL**. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-35 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 1-35 is/are rejected.

7) Claim(s) _____ is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.

 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892) 4) Interview Summary (PTO-413)
2) Notice of Draftsperson's Patent Drawing Review (PTO-948) Paper No(s)/Mail Date. ____ .
3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date ____ .
5) Notice of Informal Patent Application (PTO-152)
6) Other: ____ .

DETAILED ACTION

Claims 1-35 are presented for examination on the merits.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-35 are rejected under 35 U.S.C. 102(e) as being anticipated by Hurtado et al. (hereinafter Hurtado), US Patent Application Publication 2003/0105718 A1.

As per the following claims, Hurtado discloses:

1. A method of revoking a device, the method comprising: receiving a certificate from the device, the certificate including one or more fields, at least one of the fields holding a signature; attempting to verify the signature; receiving a revocation list from a source, the revocation list identifying one or more data on the certificate as valid or invalid, the data including at least one of the fields of the certificate; and if one or more signatures identified unsuccessfully verified and one or more data is identified as invalid, preventing the transmission of a session key to the device, the session key being required to establish a secure communication channel (figures 1-6 and associated text).

2. The method of claim 1 wherein the revocation list is evaluated upon file access (paragraph 368-374).
3. The method of claim 2 wherein the revocation list is stored upon file creation (paragraph 368-374, 458).
4. The method of claim 1 wherein each file has one revocation list, a plurality of files with a plurality of revocation lists having duplicative entries (paragraph 368-374, 458).
5. The method of claim 4 wherein the duplicative entries among a plurality of revocation lists are limited by centrally storing the details and providing each file with a list of identifiers or pointers that reference a location of complete details regarding revocation information (paragraph 368-374, 458).
6. The method of claim 5 wherein the revocation information may be stored by revocation nodes and the revocation list associated with a file may be stored as a list of revocation node identifiers (figures 5, 6 and associated text; paragraph 368-374, 458).
7. The method of claim 6 wherein each revocation node consists of a list of clauses and a rule for combining the clauses for determining the evaluation for the node (figures 5, 6 and associated text; paragraph 368-374, 458).

8. The method of claim 7 wherein the revocation results are finalized by one of get play key, play, record, copy, open, close, create, get metadata and set metadata (figures 5,6, 8-10 and associated text).

9. The method of claim 1 wherein the revocation list is stored on media along with the file (figure 5, 6 and associated text; paragraph 368-374, 458).

10. The method of claim 1 wherein the revocation list is copied onto each device (figures 1-5 and associated text; paragraph 368-374, 458).

11. The method of claim 1 wherein the revocation list is maintained by a server such that content rendering devices communicating with a server receive updated revocation lists directly to the device (figures 1D and associated text; paragraph 368-374, 458).

12. The method of claim 1 wherein a plurality of revocation lists are stored on media on a file-by-file basis, such that one or more files on the media may have a revocation list associated with the file (paragraph 368-374, 458).

13. The method of claim 12 wherein the revocation list is accessed during one of a file access process and a combination of both an authentication and a file access process (paragraph 368-374, 458).

14. The method of claim 1 wherein the revocation list includes a poison pill that prevents a content rendering device from operating (paragraph 789, 912).
15. The method of claim 1 wherein the revocation list is updated when the content rendering device is connected to a server (paragraph 368-374, 458).
16. The method of claim 1 wherein revocation of a content rendering device includes at least revocation of one or more public keys, the revocation of a public key revoking any corresponding signature (paragraph 368-374, 458).
17. The method of claim 1 wherein the revocation list is maintained as an object within the file system on the media with a distinct handle (paragraph 368-374, 458, 951, 1055).
18. The method of claim 1 wherein the revocation information is centrally located (paragraph 368-374, 458).
19. The method of claim 1 wherein the source is one of a portable medium and firmware (figures 1-6 and associated text).
20. The method of claim 1 wherein the information as to whether certificates and/or public keys have been revoked is stamped on the media (paragraph 368-374, 458).

21. The method of claim 1 wherein the device is one of an engine, a component that embeds an engine, a third party digital rights management protocol, an application running in an open computing environment, and a clearinghouse server, the certificate identifying one or more secure application programming interfaces (APIs) for which an application operable with the device may have access (figures 1-6 and associated text).
22. The method of claim 1 wherein the certificate is signed by a private key assigned according to a class of device, the class of device including engines, components embedding an engine with no external digital input/output port, components embedding an engine with digital input/output ports, and host applications not embedding an engine (paragraph 229 and associated figure).
23. The method of claim 1 wherein the data in the certificate specifies one or more of a product category, a product line, a model, a revision and a serial number of the device (paragraph 457).
24. The method of claim 23 wherein source validation data is compared with the data on the certificate to identify as invalid one or more of the product category, the product line, the model, the revision and the serial number of the host (paragraph 462-463).
25. The method of claim 24 wherein the certificate includes one or more of the following fields: certifying authority identifier, version, certifying authority public key, certifying authority public key identifier, exposed methods, company, model identifier, revision, metadata identifier, host

signature public key, certifying authority signature, serial number, protocol key and host signature, wherein the certifying authority signature verifies one or more of the fields in the certificate and the host signature verifies one or more of the fields in the certificate (paragraphs 229, 251, 293).

26. The method of claim 1 wherein the certificate enables an entity receiving the certificate to control quality of the device by invalidating devices that are false or have latent defects (figures 6-10 and associated text).

27. The method of claim 25 wherein the certificate further includes fields provided by a device manufacturer, including the device public key, wherein the device public key is signed by a private key (pages 18-23).

28. The method of claim 25 wherein one or more of the product category, the product line, the model, the revision and the serial number of the host are provided to a certificate creator after the host passes a qualification procedure (paragraphs 157, 194).

29. The method of claim 1 wherein the certificate specifies one or more certificate classes, the certificate classes providing a set of methods that may be exposed after the transmitting the session key (paragraphs 880-884).

30. The method of claim 29 wherein the set of methods includes digital rights management

(DRM) methods, copy, record, play, read secure metadata, write secure metadata, and unlock, the methods operable according to a type of the device (paragraph 10).

31. The method of claim 30 wherein: the unlock method is associated with a clearinghouse server; the copy method is associated with one of an engine and a first DRM application operable with a second DRM application; and the import method is associated with one or more of a player, a mastering tool, a kiosk, and a clearinghouse server (figures 1-6 and associated text).

32. The method of claim 1 wherein each of the fields hold 326-bit values for 163-bit elliptic curve cryptography (paragraphs 52, 193-197, 248-256).

Claims 33-35 are directed to a computer medium; apparatus and a computer engine of the above claimed invention and are rejected as above.

Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

- US PAP 2002/0107803 A1.
- U.S. Patent 6,418,421 B1.
- U.S. Patent 6,389,538 B1.
- U.S. Patent 6,389,403 B1.
- US PAP 2003/0046238 A1.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Bradley Bayat whose telephone number is 703-305-8548. The examiner can normally be reached on Tuesday-Friday during normal business hours.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell can be reached on 703-305-9768. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

bbb

John W. Hayes
JOHN W. HAYES
PRIMARY EXAMINER